APLICACIÓN INFORMÁTICA FORENSE PARA EL ANÁLISIS DE DISPOSITIVOS TECNOLÓGICOS

AUTORES: Carlos Andrés Villacreses Parrales[1]
Jennifer Elizabeth Chóez Calle[2]
Victor Antonio Figueroa Castillo[3]
Jennifer Xiomara Barreto Pin[4]

DIRECCIÓN PARA CORRESPONDENCIA: (carlosvillacresesparrales23@gmail.com)

Fecha de recepción: 26/02/2021

Fecha de aceptación: 28/05/2021

RESUMEN

El presente trabajo de investigación se fundamentó en dar a conocer el uso correcto de software que se utilizan para el análisis y extracción de la información existente en los dispositivos tecnológicos, mediante aplicaciones que se emplean en la informática forense; así mismo hacer el uso correcto de las mismas, conociendo sus ventajas y desventajas; a su vez emplear los requerimientos necesarios para su implementación y posterior utilización. Dentro de la investigación se utilizaron diferentes métodos predominando el método análisis-síntesis, histórico-lógico, deducción–inducción, referencial-bibliográfico; los cuales fueron de gran ayuda para fundamentar la investigación. Estas aplicaciones se basan primordialmente en analizar y encontrar incidencias que se encuentren presentes en los dispositivos tecnológicos y de tal manera conocer la situación actual de la información, teniendo presente que la información se obtiene a través de archivos borrados, alterados o actividades desarrolladas en internet como lo son: los correos electrónicos, entre otros; determinando un patrón de comportamiento del control del ordenador. Teniendo como impacto el contribuir en la adquisición de conocimientos en los lectores sobre las aplicaciones forenses que se emplean para el estudio y análisis de la información en la informática forense, siendo de gran ayuda ya sea en el ámbito personal, laboral o educativo.

PALABRAS CLAVE: análisis forense; dispositivo; información; aplicación.

[1]Profesional en formación de la Carrera Tecnologías de la Información. Facultad de Ciencias Técnicas.Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador.https://orcid.org/0000-0002-4048-4316. E-mail: carlosvillacresesparrales23@gmail.com
[2]Profesional en formación de la Carrera Tecnologías de la Información. Facultad de Ciencias Técnicas.Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador.https://orcid.org/0000-0001-6051-2479. E-mail:jenniferelizachoezcalle@gmail.com
[3]Profesional en formación de la Carrera Tecnologías de la Información. Facultad de Ciencias Técnicas.Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador.https://orcid.org/0000-0002-7810-9730. E-mail: victor-fige@outlook.com

[4]Profesional en formación de la Carrera Tecnologías de la Información. Facultad de Ciencias Técnicas.Universidad Estatal del Sur de Manabí. Jipijapa, Manabí, Ecuador.https://orcid.org/0000-0002-9610-8002. E-mail: jenniferbarretopin@gmail.com

COMPUTER FORENSIC APPLICATION FOR THE ANALYSIS OF TECHNOLOGICAL DEVICES

ABSTRACT

The present research work was based on making known the correct use of software used for the analysis and extraction of existing information in technological devices, through applications that are used in forensic computing; likewise make the correct use of them, knowing their advantages and disadvantages; In turn, use the necessary requirements for its implementation and subsequent use. Within the research, different methods were used, predominating the analysis-synthesis, historical-logical, deduction-induction, referential-bibliographic method; which were of great help to support the investigation. These applications are based primarily on analyzing and finding incidents that are present in the technological devices and in such a way to know the current situation of the information, keeping in mind that the information is obtained through deleted, altered files or activities developed on the Internet as they are: emails, among others; determining a pattern of computer control behavior. Having as impact the contribution in the acquisition of knowledge in the readers about the forensic applications that are used for the study and analysis of the information in forensic computer science, being of great help either in the personal, labor or educational field.

KEYWORDS: application; device; information; forensic analysis.

INTRODUCCIÓN

La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en soportes informáticos, se trata de una práctica cada vez más habitual debido al uso que actualmente todos realizamos de las nuevas tecnologías. Según Hobbes, en El Leviatán, quien puso en circulación la idea de “quien tiene la información tiene el poder”; en pocas palabras conviene decir que la información no es conocimiento.

Existen muchas formas de perder información, ya sea involuntariamente como: daños en los equipos, accidentes, desastres naturales, entre otros o intencionalmente como: robo, sabotaje, violaciones a la integridad de la información, por mencionar algunos.

Se pretende que los lectores adquieran los conocimientos necesarios del uso correcto de software empleados en el análisis forense para aquellos que hacen uso de ciertas actividades que son de gran importancia.

La informática forense está construida sobre una serie de metodologías diseñadas para guiar las investigaciones y los procesos de búsqueda de pruebas, de tal forma que se pueda asegurar que la información no ha sido modificada o dañada en el proceso o durante la investigación.

Dentro de las etapas de proceso como lo son: la incautación, la adquisición forense, el análisis y la producción de los datos recogidos; así mismo como lo es la adquisición lógica, física y de sistemas de ficheros en los ordenadores y dispositivos móviles.

El utilizar los diferentes softwares en los ordenadores y dispositivos móviles favorece a obtener información no solo de gran importancia, sino que a su vez; poder realizar una copia exacta de la misma, ya sean de llamadas, correos electrónicos, documentos, videos, fotos e incluso información eliminada previamente.

El software OSForensics en la actualidad se ha implementado en los ordenadores para el análisis de la información; mencionando así para los dispositivos móviles el software OxygenForensic, los cuales realizan procesos muy similares, almacenando gran información que sirven para su posterior estudio.

Teniendo, así como objetivo principal, brindar a los lectores una investigación relacionada con el uso correcto de software que se utilizan para el análisis y extracción de la información existente del ordenador y dispositivos móviles

El impacto que se obtuvo en los usuarios fue aceptable por lo que es una técnica muy eficaz, eficiente y además muy innovadora que permitirá obtener información de ordenadores y así mismo de dispositivos móviles, siempre y cuando se haga uso de un software apropiado y de manera correcta.

DESARROLLO

La informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computeranalysis and response team), o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense". (Mitrik, 2018)

A partir de que se inició la informática forense en el año 1980 los ordenadores se transformaron en una opción más factible obtener por los diferentes usuarios o personas, así mismo surgen los fraudes y ocurre perdida de información, así es como surgió una aplicación creada por el FBI denominada como CART, la cual le da el nombre a la informática forense en la actualidad.

El análisis informático forense es un área de la seguridad informática que evoluciona en forma constante con los avances tecnológicos y en paralelo con el perfeccionamiento de los ataques informáticos. Estos aplicativos, al igual que la rama de la informática que soportan, siguen evolucionando al paso de la tecnología para lograr mejores resultados. (Arnedo Blanco, 2014)

Con el pasar de los días las tecnologías avanzan de tal manera también lo hace el análisis forense en el ámbito de la seguridad informática de forma que se perfecciona para que no existan ataques informáticos, permitiendo no solo que se conozcan las incidencias, fraudes ocurridos en diferentes índoles de dispositivos tecnológicos, sino que a su vez conocer información ya eliminada.

El ecosistema de los dispositivos móviles ha evolucionado de una manera vertiginosa en los últimos años provocado principalmente por su adopción masiva por parte de los usuarios, los

cuales llegan a tener de manera simultánea varios terminales con diferentes objetivos: uso profesional, uso personal, etc. Hay estimaciones que indican que en la actualidad hay más de 7.500 millones de dispositivos móviles, lo que supone una cifra superior al de la población mundial. (Martínez, 2015)

Aproximadamente 7.500 millones de dispositivos móviles han evolucionado de manera satisfactoria provocando una adquisición masiva de los usuarios, lo cual usarlos de manera adictiva tiene muchas consecuencias; Es por ello que surgen diferentes aplicaciones forenses que permiten que prevalezca la información ya sean archivos, documentos, archivos multimedia, entre otros, haciendo el uso correcto de estas aplicaciones se podría implementar es los dispositivos tecnológicos de manera satisfactoria evitando la perdida de información.

Características de las herramientas forenses

Las características de las herramientas forenses profesionales varían mucho dependiendo de la rama del análisis forense y el mercado al que están orientados.

- ✓ Hash de disco completo para poder confirmar que los datos no han cambiado (normalmente se utiliza una herramienta para adquirir y otra para confirmar el hash de disco).
- ✓ Localizadores de rutas exactas.
- ✓ Borrar los sellos de fecha y hora.
- ✓ Tiene que incluir una característica de adquisición.
- ✓ Búsqueda y filtrado de artículos.
- ✓ La capacidad de cargar copias de seguridad de iOS y analizar sus datos

HERRAMIENTAS Y EQUIPOS DE INFORMÁTICA FORENSE PARA ORDENADORES

Las diferentes herramientas que existen que son empleadas en lo cotidiano por investigadores y especialistas en informática forense son las siguientes:

BlackBag Technologies: es la herramienta forense para Mac, herramienta de inspección para Windows también analiza todos los dispositivos iOS, así como Android.

AccessData: Proporciona el filtrado y la búsqueda de dispositivos Móviles y Ordenadores, que son más rápidos que con cualquier otra solución.

Guidance Software: desarrolla EnCaseForensic Software que es una herramienta de análisis forense para PC, usada para encontrar pruebas de pornografía infantil.

MagnetForensics: Desarrollada por un ex oficial de policía y programador, MagnetForensics es una plataforma completa de investigación digitalde teléfonos donde sea posible (la mayoría de Android y iPhone 4 e inferior, y BlackBerry).

X-Ways: Hacen un trabajo fantástico cuando se trata de imágenes de disco, clonación de disco, reconstrucción de RAID virtual, análisis de unidad de red remota, acceso remoto a RAM, acceso a almacenamiento en la nube.

Disk Drill: Utilizada para recuperar documentos, imágenes, archivos de vídeo y otros tipos de datos de una variedad de dispositivos de almacenamiento diferentes.

OSForensic: es una pieza clave en investigaciones forenses digitales (digital forensics, como se conoce en inglés), un todo en uno que permite localizar pistas, mirar en el interior de archivos y sus cabeceras y, finalmente, organizar e indexar todos los datos hallados para un tratamiento posterior y su presentación. (Lance, 2018).

Funcionamiento deOSForensic

OSForensics puede ser de mucha utilidad, ya que puede mostrarnos todas las actividades que ha realizado otro usuario en nuestro equipo. Para ello trabaja el análisis de la información mediante en 3 fases que permiten que la misma se desarrolle de manera correcta.

- **Descubrimiento:** Es capaz de extraer contraseñas, descifrar archivos y recuperar elementos borrados de diferentes sistemas de archivos: Windows, Mac y Linux.
- **Identificación:** Se analizan todos los archivos y permite crear una línea de tiempo (timeline) de toda la actividad del usuario, para presentarla en orden cronológico.
- **Administración:** Permite organizar todas nuestras evidencias en un guión ordenado, incorporando los datos del examinador forense.

Ventajas de OSForensic

- Soporte para OCR en Windows 10
- Informes cifrados en PDF
- Mejora x3 en velocidad de indexado, añadiendo soporte multi-hilo, disco RAM y bypass de pre-escaneo
- Salto desde el Visor de disco en bruto al registro MFT
- Función de quickhashing
- Soporte para EFS o Encrypted File System
- Incorpora la última versión de VolatilityWorkbench con soporte para Mac y Linux
- Recuperación de claves de Bitlocker
- Función de auto-descubrimiento mejorada
- Extracción de vídeos en formato MP4 desde webs como YouTube (Alejandro, 2018)

ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Desde que el móvil ha llegado a formar parte cotidiana de nuestras vidas, se ha convertido en un compañero del que difícilmente nos desprendemos ya sean para comprar entradas, como reproductor de música, como medio de comunicación con nuestro entorno, entre otros. (Abogacia Española, 2017)

En vista de que los dispositivos móviles se han convertido en una necesidad cotidiana la realización de un análisis forense permite conocer la información que haya sido adquirido por otros de manera ilegal o accidentalmente eliminada de algún dispositivo tecnológico. Para detallar con más precisión el realizar un análisis a los dispositivos mediante aplicaciones forenses permite que la información se resguarde de manera segura, lo cual en los diferentes ámbitos ya sea personal, laboral o profesional se puede convertir en una gran herramienta que facilitara enormemente procesos o actividades cotidianas.

Funcionamiento en móviles

A grandes rasgos existen 3 métodos distintos de extracción de evidencias: adquisición física, adquisición del sistema de ficheros y adquisición lógica.

Adquisición física: Consiste en realizar una réplica idéntica del original por lo que se preservan la totalidad de las evidencias potenciales en archivos que han sido eliminados.

Adquisición lógica: Consiste en realizar una copia de los objetos almacenados en el dispositivo. Para ello, se utilizan los mecanismos implementados de manera nativa por el fabricante, es decir, aquellos que son utilizados de manera habitual para sincronizar el terminal con un ordenador.
Adquisición del sistema de ficheros: permite obtener todos los ficheros visibles mediante el sistema de ficheros, lo que no incluye ficheros eliminados o particiones ocultas.

¿Qué es lo que se puede obtener de un dispositivo móvil en caso de un análisis forense?
Todos estos datos:
Se pueden recuperar todas las llamadas, mensajes SMS, y de mensajería instantánea, emails, agenda de contactos, el historial de navegación, calendario, etc. incluso aunque estos se hayan borrado.
Se pueden recuperar las fotos, vídeos y cualquier tipo de archivo que haya sido almacenado en el dispositivo (incluso aunque se hayan borrado), pudiendo extraer incluso información de en dónde se tomó dicha foto, o dicho vídeo gracias a los datos de ubicación GPS incrustados en forma de metadatos en dicho material multimedia.
Se puede recuperar fácilmente los trayectos que efectuó dicha persona, gracias a:

- Los datos que pueden proporcionar los operadores de telefonía mediante los registros que ellos tienen de conexión del terminal a las diferentes antenas de telefonía;
- Los datos de posicionamiento que proporcionan las fotos y los vídeos que se han realizado con la cámara del dispositivo móvil;
- Los registros del GPS que usan algunas aplicaciones para su funcionamiento como Uber, Google Maps, Waze, Facebook, Telegram, WhatsApp, entre otros.

Se pueden reconstruir incluso las capturas de las últimas pantallas que aparecieron en el terminal antes de su análisis forense.
Se puede acceder incluso a lo que se ha estado escribiendo desde dicho dispositivo si el teclado del dispositivo deja algún rastro.

La mayoría de terminales están cifrados con la contraseña o patrón, por ello lo primero que tienen que hacer las herramientas forenses es acceder a dicha contraseña y/o patrón de desbloqueo para poder acceder a dicho contenido. Para ello hacen lo siguiente:

- Clonan el dispositivo original para que, en el caso de que se llegue al límite de intentos impuesto por el fabricante al introducir la contraseña/patrón de desbloqueo, no se destruya el contenido de este.
- Se ha demostrado que, para acceder a una contraseña de 4 dígitos, con un ataque de fuerza bruta (es decir probando todas las combinaciones) se tardan unas 16 horas en poder averiguarla. (Abogacia Española, 2017)

Herramientas usadas para el análisis en móviles
Genéricas:

Open Source Android Forensics es un framework que se distribuye mediante una imagen de máquina virtual que reúne varias herramientas que permiten analizar aplicaciones para dispositivos móviles, incluyendo análisis tanto estático como dinámico o incluso para realizar un análisis forense.

Específicas

Android Data Extractor Lite (ADEL) es una herramienta desarrollada en Python que permite obtener un flujograma forense a partir de las bases de datos del dispositivo móvil. Para poder realizar el proceso, es necesario que el dispositivo móvil esté rooteado o tener instalado un recovery personalizado.

Pago

OxygenForensic Suite es capaz de obtener información de más de 10.000 modelos diferentes de dispositivos móviles e incluso obtener información de servicios en la nube e importar backups o imágenes.

OXYGEN FORENSIC
Oxygen Detective Forense está diseñado específicamente para análisis forense, búsqueda de pruebas y presentación de informes. La herramienta puede imprimir informes y exportarlos a los formatos de archivo más populares. (Danysoft, 2019)

Ventajas

- Independiente para la visualización y el intercambio de la información recogida con otros productos.
- Acceder al conjunto completo de pruebas.
- Análisis de datos borrados.
- examinar comunicaciones de sospechosos.
- Localizar todos los tipos de pruebas con búsqueda integrada.

Características

Se puede recuperar fácilmente los trayectos que efectuó dicha persona, gracias a:

- Los datos que pueden proporcionar los operadores de telefonía mediante los registros que ellos tienen de conexión del terminal a las diferentes antenas de telefonía.
- Los datos de posicionamiento que proporcionan las fotos y los vídeos que se han realizado con la cámara del dispositivo móvil.
- Los registros del GPS que usan algunas aplicaciones para su funcionamiento como Uber, Google Maps, Waze, Facebook, Telegram, WhatsApp. (Jiménez, 2017)

MATERIALES Y MÉTODOS

Los materiales que se llevaron a cabo para la investigación fueron: diversas fuentes bibliográficas la cual permitió sustentar la investigación, así mismo como las revistas, artículos; entre otros.

En cuanto al desarrollo de la investigación se utilizaron métodos científicos tales como: métodos teóricos predominando el histórico-lógico para determinar los antecedentes presentes en la investigación sobre el análisis forense desde su inicio hasta la actualidad; el análisis–síntesis para analizar y sintetizar diversas opiniones de diferentes artículos; referencial-bibliográficas para las fuentes de la investigación y tener una base de sustentación fundamentada.

RESULTADOS

Dentro del análisis forense que se realiza a los dispositivos digitales se debe de seguir un proceso según expertos; el caso se detalla a continuación es un análisis a un computador personal que se obtuvo como evidencia en un proceso delictivo en España en el año 2016, realizado por Diego F. González Acevedo. El procedimiento que se debe de seguir se detalla en el siguiente diagrama:

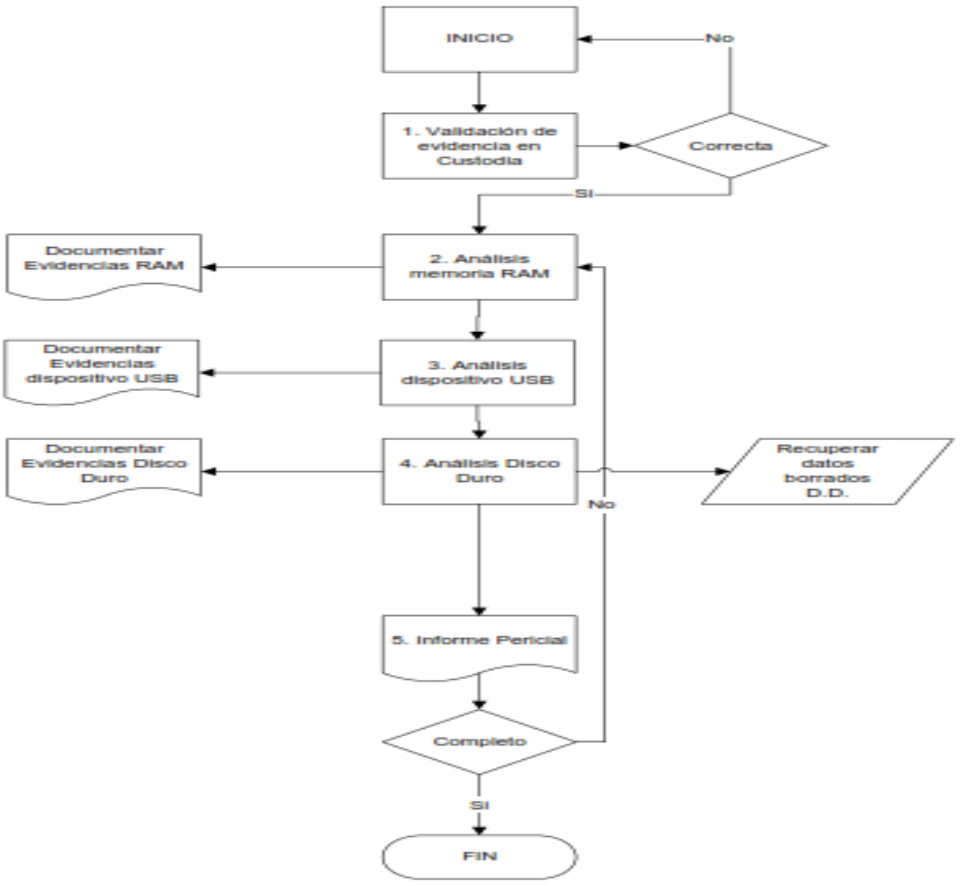

Figura 1: Diagrama de procedimiento del análisis forense

Fuente: Obtenidos de la Web - El diagrama puede variar según el perito

Para el análisis forense se debe de hacer una planificación de inicio y de finalización de cada uno de los procesos que se nombraron en el diagrama anterior.

La herramienta que se utilizó para el análisis es **OSForensics**, en el cual se realizó los siguientes procedimientos:

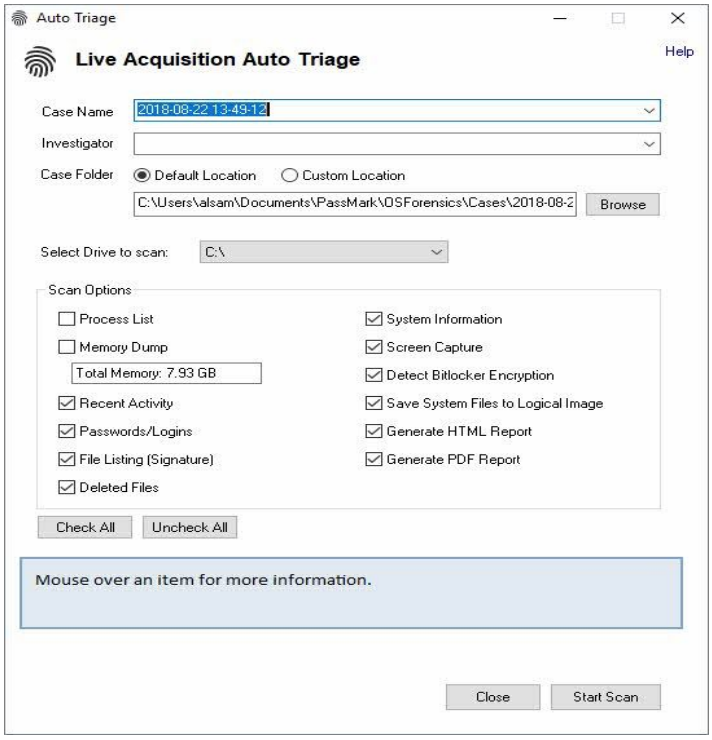

Figura 2: Pantalla inicial de OSRorencis

La opción **Auto Triage** recopila importante información contextual (información de sistema) e incluso nos presenta los datos en un informe final.

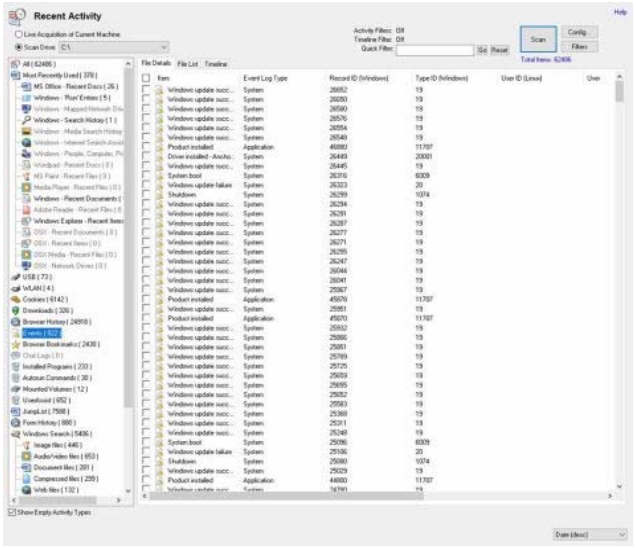

Figura 3: Auto Triage – Información recopilada del análisis

La opción **RecentActivity** aparecerán toda suerte de archivos abiertos recientemente, jumplists, comandos ejecutados, programas instalados, favoritos de navegadores, descargas de archivos,

cookies, unidades de disco montadas, búsquedas de Windows Search, archivos prefetch y un largo etcétera.

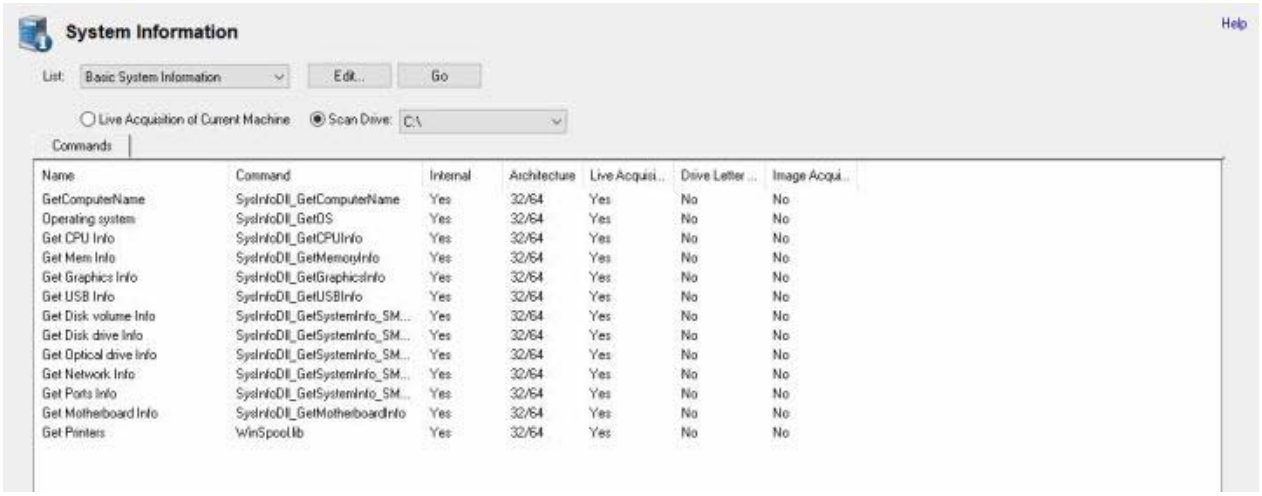

Figura 4: RecentActivity

Con la opción **System Information** permite tener información detalla del ordenador y cada uno de sus componentes.

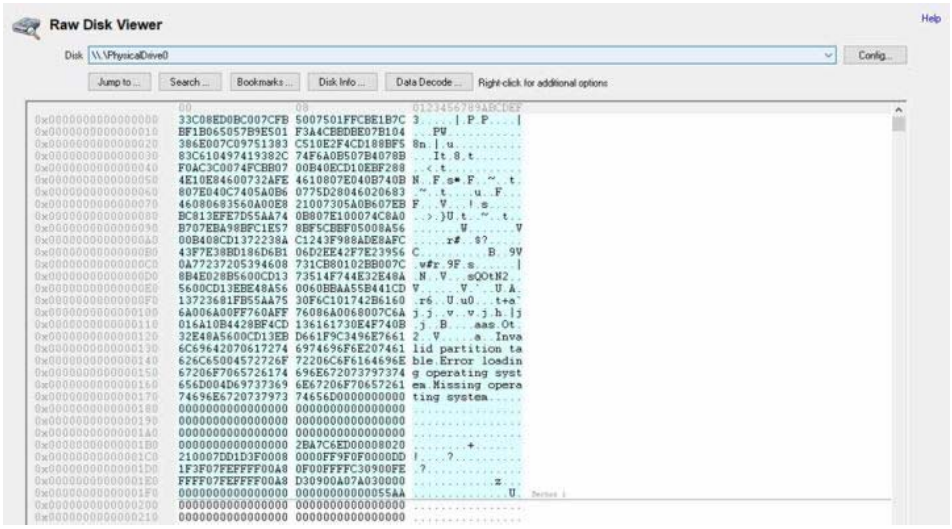

Figura 5: System Information – Información detallada del ordenador y sus componentes

El módulo Raw Disk Vieweres capaz de leer más allá de directorios o sistemas de archivos, ya que accede al nivel más bajo posible.

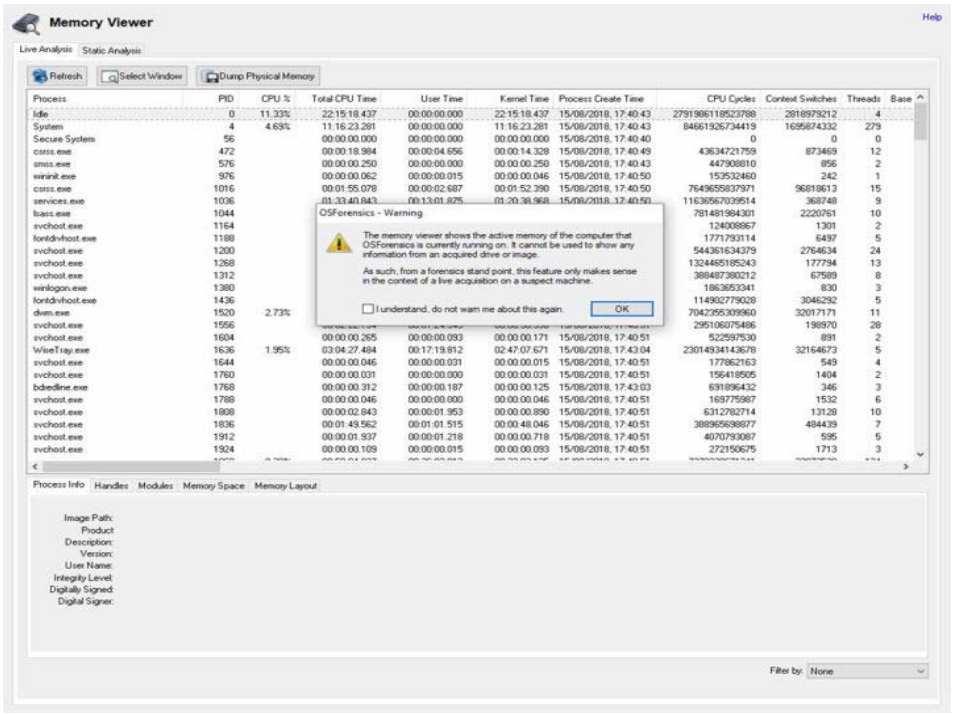

Figura 6: Raw Disk Viewer – Acceso a nivel bajo de los directorios

Este módulo Memory Viewer diseñado específicamente para analizar memoria volátil del sistema nos ofrece la opción de capturar en modo Live (usada por el sistema encendido o "vivo") así como analizar un volcado de memoria previamente capturado.

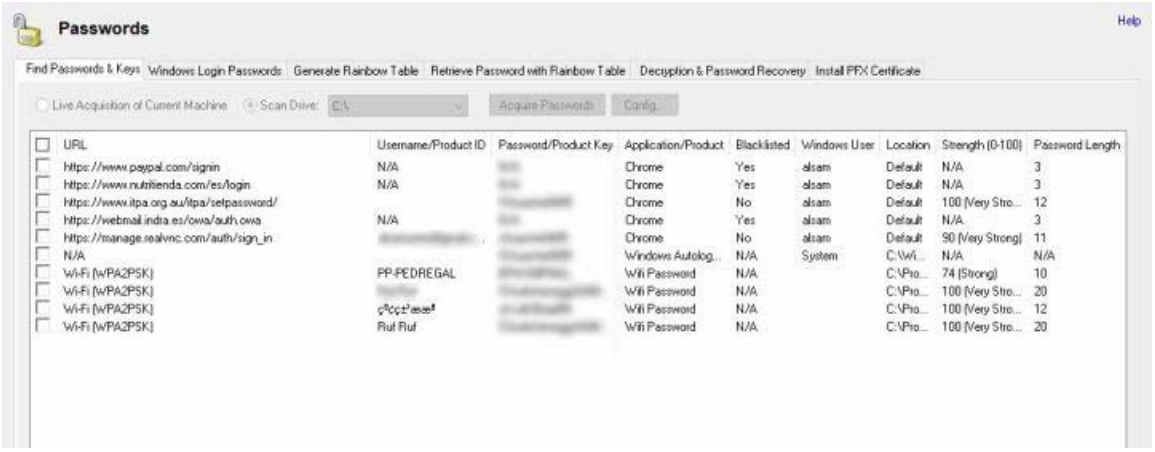

Figura 7: MemoryViewer – Análisis de la memoria volátil del sistema

El módulo Passwords permite obtener contraseñas de diversas fuentes como navegadores, sistemas operativos (Windows login) e intentar atacar los hashes de estas mediante Rainbow tables. También permite el descifrado de documentos de ofimática.

Con la utilización de aplicaciones informáticas forenses en los dispositivos tecnológicos se pretende que los lectores conozcan las nuevas formas de recuperación de sus archivos, correos entre otros; y a su vez adquieran conocimientos del cómo usarlas, así mismo de cómo se encuentra estructurado.

El impacto que se obtuvo en diferentes lectores fue aceptable, e incluso los motivó a profundizar el tema conocer en que tecnologías se pueden realizar un análisis forense, así mismo sus beneficios como sus requerimientos para su utilización.

DISCUSIÓN

Figura 8: Delitos Informáticos en Ecuador

Figura 9: Delitos Informáticos en Ecuador realizados en dispositivos móviles

Según las estadísticas que se han desarrollado desde el año 2009 hasta el año 2015 se contabilizaron 10,025 delitos, en las ciudades que con más frecuencia se observaron estas incidencias son: Pichincha con un 47,38%; Guayas con 27,57%; El Oro con 5,24%. No obstante, en los años 2017 hasta la actualidad se han registrados delitos cibernéticos a dispositivos móviles aumentando sus cifras en el año 2017-2018. Teniendo presente que no todos los casos que se han presentado han sido denunciados ni previamente todos resueltos.

Hoy en día las Instituciones que hacen justicia están haciendo uso de este tipo de aplicaciones para resolver incidencias cibernéticas mas no obstante se rastrean los diferentes dispositivos tecnológicos mediante aplicaciones forenses para así resolver lo que se presenta en el mundo actual con mayor frecuencia.

CONCLUSIONES

Se colige que la integración de la data mining en el entorno empresarial es de gran ayuda debido a que no solo se conocer y obtener patrones, comportamiento es decir información relevante, sino que a la vez se aplican estrategias que posterior a utilizarlas podría tener un gran crecimiento la organización, aplicando redes, patrones, inteligencia artificial y así recopilar los datos de grandes bases de datos, como los gustos o tendencias de los clientes y el entorno en el que se encuentran.

Las técnicas como lo son las redes neuronales, la clasificación de la información, los clústeres de los datos que se tienden a ser comunes como las características de los clientes, productos y así emplear las herramientas como lo son la verificación y descubrimiento, es decir predecir y detectar lo que puede afectar o mejorar en las empresas.

REFERENCIAS BIBLIOGRÁFICAS

Abogacia Española. (28 de Julio de 2017). *Consejo general de la abogacia española*. Obtenido de Análisis forense de los dispositivos móviles: https://www.abogacia.es/2017/07/28/analisis-forense-de-los-dispositivos-moviles/

Alejandro. (23 de Agosto de 2018). *protegermipc.net*. Obtenido de OsForensics, una potente herramienta de informática forense para Windows: https://protegermipc.net/2018/08/23/osforensics-herramienta-informatica-forense-windows/

Arnedo Blanco, P. (11 de Marzo de 2014). *reunir.unir.net.* Obtenido de Herramientas de analisis forense en la investigacion de delitos informaticos : https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

Danysoft. (05 de Enero de 2019). *danysoft.com*. Obtenido de Oxygen Detective Forense: https://www.danysoft.com/oxygen-forensics/

Jiménez, I. (28 de Julio de 2017). *abogacia.es*. Obtenido de Análisis forense de los dispositivos móviles: https://www.abogacia.es/2017/07/28/analisis-forense-de-los-dispositivos-moviles/

Lance. (24 de Febrero de 2018). *cleverfiles.com*. Obtenido de Lista de las mejores herramientas de informática forense, Recuperación forense de datos, Análisis forense digital: https://www.cleverfiles.com/howto/es/computer-forensic.html

Martínez, A. (12 de Noviembre de 2015). *incibe-cert.es*. Obtenido de Introducción al análisis forense en móviles: https://www.incibe-cert.es/blog/introduccion-analisis-forense-en-moviles

Mitrik, K. (29 de Noviembre de 2018). *informaticaforense1.blogspot.com*. Obtenido de Historia Informática Forense: http://informaticaforense1.blogspot.com/2013/11/historia-informatica-forense.html